

07/31/00
JC760 U.S. PTO

Please type a plus sign (+) inside this box → ☐

PTO/SB/05 (12/97)
Approved for use through 09/30/00. OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.

K35A0638

Total Pages

25

First Named Inventor or Application Identifier

CHRISTOPHER L. HAMLIN

Express Mail Label No.

EI266880172US

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

ADDRESS TO:

Assistant Commissioner for Patents
Box Patent Application
Washington, DC 20231

1. ☒ Fee Transmittal Form
(Submit an original, and a duplicate for fee processing)
2. ☒ Specification [Total Pages **18**]
(preferred arrangement set forth below)
- Descriptive title of the Invention
 - Cross References to Related Applications
 - Statement Regarding Fed sponsored R & D
 - Reference to Microfiche Appendix
 - Background of the Invention
 - Brief Summary of the Invention
 - Brief Description of the Drawings (if filed)
 - Detailed Description
 - Claim(s)
 - Abstract of the Disclosure
3. ☒ Drawing(s) (35 USC 113) [Total Sheets **5**]
X Formal _ Informal
4. Oath or Declaration [Total Pages **1**]
- a. ☐ Newly executed (original or copy)
 - b. ☐ Copy from a prior application (37 CFR 1.63(d))
(for continuation/divisional with Box 17 completed)
(Note Box 5 below)
 - i. ☐ DELETION OF INVENTOR(S)
Signed statement attached deleting
inventor(s) named in the prior application,
see 37 CFR 1.63(d)(2) and 1.33(b).
5. ☐ Incorporation By Reference (useable if Box 4b is checked)
The entire disclosure of the prior application, from which a
copy of the oath or declaration is supplied under Box 4b,
is considered as being part of the disclosure of the
accompanying application and is hereby incorporated by
reference therein.

6. ☐ Microfiche Computer Program (Appendix)
7. Nucleotide and/or Amino Acid Sequence Submission
(if applicable, all necessary)
- a. ☐ Computer Readable Copy
 - b. ☐ Paper Copy (identical to computer copy)
 - c. ☐ Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

8. ☐ Assignment Papers (cover sheet & document(s))
9. ☐ 37 CFR 3.73(b) Statement ☐ Power of Attorney
(when there is an assignee)
10. ☐ English Translation Document (if applicable)
11. ☐ Information Disclosure Statement (IDS)/PTO-1449 ☐ Copies of IDS Citations
12. ☐ Preliminary Amendment
13. ☒ Return Receipt Postcard (MPEP 503)
(Should be specifically itemized)
14. ☐ Small Entity ☐ Statement filed in prior application,
Statement(s) Status still proper and desired
15. ☐ Certified Copy of Priority Document(s)
(if foreign priority is claimed)
16. ☐ Other: _____

17. If a CONTINUING APPLICATION, check appropriate box and supply the requisite information:

☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No: _____/_____

18. CORRESPONDENCE ADDRESS

☐ Customer Number or Bar Code Label

(Insert Customer No. or Attach bar code label here)

or ☒ Correspondence address below

NAME	WESTERN DIGITAL CORPORATION				
	Milad G. Shara, Esq. - Reg. 39,367				
ADDRESS	8105 IRVINE CENTER DRIVE				
	PLAZA 3				
CITY	IRVINE	STATE	CALIFORNIA	ZIP CODE	92618
COUNTRY	U.S.A.	TELEPHONE	(949) 932-5676	FAX	(949) 932-5633

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231.

**A COMPUTER NETWORK COMPRISING NETWORK AUTHENTICATION
FACILITIES IMPLEMENTED IN A DISK DRIVE**

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates to computer networks. More particularly, the present invention relates to a computer network comprising network authentication facilities implemented in a disk drive.

Description of the Prior Art

Computer networks comprise a number of interconnected network devices (server computers, client computers, disk drives, printers, etc.) which communicate with one another through a network communication protocol (Ethernet, ATM, etc.). Each device is typically assigned an address which identifies the device, where the device address is used to route messages to and from the device through the network. For example, a client computer may request access to a server computer by sending a message to the server computer. The message typically comprises the address of the server computer for routing the initial message, as well as the address of the client computer for routing a reply message.

Computer networks also typically employ authentication services which manage and enforce user access rights with respect to each network device. For example, a mail server may be configured so that it is accessible only by authorized users with established accounts. The authentication facility may be implemented by each network device by storing a list of authorized users and associated authentication data (e.g., passwords). When a user sends an access request to a network device, the network device will verify that the user has the appropriate access rights. In an open environment, however, this implementation can place a substantial burden on each network device as well as complicate the administrative task required to manage the user access rights for each network device.

1 An alternative is to use an authentication server which maintains the user IDs and
2 associated authentication data in a centralized authentication database. Users requesting access
3 to a particular network device must first be authenticated by the authentication server. Once
4 authenticated, the authentication server transmits device access data to the user's client computer
5 which is then used to access the network device. This approach is employed by the Kerberos
6 authentication service developed as part of Project Athena at MIT. An overview of the Kerberos
7 authentication service is provided by William Stallings in a text book entitled *Cryptography and*
8 *Network Security*, 2nd edition, 1999, 1995 by Prentice Hall, pp. 323-353, which is herein
9 incorporated by reference.

10 FIG. 1 illustrates the Kerberos authentication service in a computer network comprising a
11 plurality of interconnected network devices including an authentication server 2, a network
12 server 4 (e.g., a mail or file server), and a local area network (LAN) 6, all of which
13 communication through a network routing facility 10. The authentication server 2 is configured
14 by a person 12 (a system administrator) with the user access data associated with each of the
15 network devices. For example, the system administrator 12 may input a plurality of user
16 identifiers and associated passwords together with the user's access rights to the plurality of
17 network devices. This information is stored in a central authentication database in non-volatile
18 memory, for example, in disk drive 14.

19 The authentication server 2 will typically authenticate the system administrator 12 before
20 allowing any modifications to the central authentication database. The system administrator 12
21 provides personal authentication data to the authentication server 2 known only to the system
22 administrator, such as a password, voiceprint, fingerprint, etc.. The authentication server 2
23 authenticates the system administrator 12 by comparing the received personal authentication data
24 to authentication data stored locally (e.g., on disk drive 14).

25 When a user (e.g., user 16) requests access to one of the network devices (e.g., network
26 server 4), the user 16 presents a user ID together with an access request to the authentication
27 server 2 through the user's client computer 18 via the network routing facility 10. The

1 authentication server 2 evaluates the authentication database to determine whether the user ID
2 has been granted the access rights requested. If so, the authentication server 2 transmits, via the
3 network routing facility 10, device access data to the user's client computer 18, and the client
4 computer 18 uses the device access data to access the network server 4.

5 The network server 4 shares a secret key with the authentication server 2 which is used to
6 enforce the access rights contained in the central authentication data base. The network server 4
7 uses the secret key to decrypt the device access data received in a device access request; if the
8 decrypted access data is authentic, then the request is serviced, otherwise the request is denied.

9 The device access data is typically encrypted when transmitted from the authentication
10 server 2 to the client computer 18, and when transmitted from the client computer 18 to the
11 network server 4. With advanced cryptography, it is extremely difficult to decipher an encrypted
12 message, even if intercepted by an attacker, without the secret key used to decrypt the message.
13 Thus, attackers are now focusing their efforts on the network devices involved in the secure
14 transactions (e.g., the authentication server, client computers, network servers, etc.) in an attempt
15 to discover the plaintext data before encryption or after decryption, or to discover information
16 that will help reveal the secret cryptographic keys. To this end, an attacker may physically probe
17 a network device using special software, such as debuggers or decompilers, or special hardware,
18 such as logic analyzers or in-circuit emulators. An attacker may also perform a remote attack on
19 a network device using a virus program which invades the device's operating system to reveal
20 protected information. For example, a virus may be attached to an email and transmitted to a
21 network device through the network routing facility 10.

22 The authentication server 2 of FIG. 1 is susceptible to physical probing attacks as well as
23 remote virus attacks since the access control management is performed by a conventional
24 operating system running on a conventional central processing unit (CPU). Similarly, network
25 devices, such as the network server 4, are susceptible to attack since they enforce access control
26 at the operating system level using a conventional CPU. In addition, the central authentication
27 database configured by the system administrator 12 as well as the cryptographic keys shared with

1 the network devices are susceptible to attack if stored in plaintext form. For example, an attacker
2 may probe the disk drive 14 attached to the authentication server 2 or the disk drive 20 attached
3 to network server 4 in an attempt to discover the user access data and/or the secret cryptographic
4 keys stored in plaintext form.

5 There is, therefore, a need to improve the security of authentication services for computer
6 networks, particularly with respect to the authentication server and the secret keys shared with
7 the network devices.

8 SUMMARY OF THE INVENTION

9 The present invention may be regarded as a computer network comprising a plurality of
10 interconnected network devices including a plurality of client computers, an authentication server
11 computer operated by a system administrator, and a disk drive connected to the authentication
12 server computer. The disk drive comprises an interface for receiving personal authentication data
13 and user access data from the system administrator, a disk for storing data, and a disk controller
14 for controlling access to the disk. An authenticator within the disk drive, responsive to the
15 personal authentication data, enables the disk controller, and cryptographic circuitry within the
16 disk drive encrypts the user access data received from the system administrator into encrypted
17 data stored on the disk.

18 In one embodiment, the user access data comprises a plurality of user identifiers and
19 corresponding access rights to the plurality of network devices.

20 The present invention may also be regarded as a computer network comprising a plurality
21 of interconnected network devices including a plurality of client computers, an authentication
22 server computer, and a disk drive connected to the authentication server computer. The disk
23 drive comprises an interface for receiving from a client computer a user ID and a user access
24 request to access a network device, and for transmitting device access data to the client computer.
25 The disk drive further comprises a disk for storing encrypted data, and a disk controller,
26 responsive to the user ID and user access request, for controlling access to the disk.
27 Cryptographic circuitry within the disk drive decrypts the encrypted data stored on the disk to

1 generate decrypted data, and the disk controller uses the decrypted data to generate the device
2 access data transmitted to the client computer.

3 In one embodiment, the encrypted data comprises encrypted user authentication data
4 corresponding to the user ID, and the cryptographic circuitry decrypts the encrypted user
5 authentication data to generate decrypted user authentication data.

6 The present invention may also be regarded as a computer network comprising a plurality
7 of interconnected network devices including a plurality of client computers, an authentication
8 server, and a disk drive. The disk drive comprises an interface for receiving an encrypted device
9 access request and for inputting/outputting user data from/to a client computer, a disk for storing
10 data, and a disk controller for controlling access to the disk. The disk drive further comprises an
11 internal drive key, and a secret device key shared with the authentication server, the secret device
12 key stored in encrypted form. Cryptographic circuitry within the disk drive, responsive to the
13 internal drive key, decrypts the encrypted secret device key to generate a decrypted secret device
14 key, and an authenticator within the disk drive, responsive to the decrypted secret device key,
15 authenticates the device access request.

16 In one embodiment the encrypted secret device key is stored on the disk, in another
17 embodiment the encrypted secret device key is configured during manufacture of the disk drive,
18 and in yet another embodiment the disk drive transmits the encrypted secret device key to the
19 authentication server.

20 BRIEF DESCRIPTION OF THE DRAWINGS

21 FIG. 1 shows a conventional computer network comprising a plurality of interconnected
22 network devices, including an authentication server for implementing access management at the
23 operating system level using a conventional CPU.

24 FIG. 2 is a computer network according to an embodiment of the present invention
25 comprising a plurality of interconnected network devices, including an authentication server for
26 implementing access management within a disk drive connected to the authentication server.

27 FIG. 3 shows a disk drive according to an embodiment of the present invention

1 comprising an interface for receiving personal authentication data identifying a person (e.g., a
2 system administrator) and user access data for accessing the plurality of network devices,
3 wherein the user access data is stored in encrypted form on a disk.

4 FIG. 4 shows a disk drive according to an embodiment of the present invention which
5 receives a user ID and a user access request from a client computer and outputs device access
6 data to the client computer. The disk drive comprises a disk controller for accessing encrypted
7 data stored on a disk, cryptographic circuitry for decrypting the encrypted data, and an
8 authenticator, responsive to the user ID, for enabling the disk controller.

9 FIG. 5 shows a disk drive according to an embodiment of the present invention which
10 receives an encrypted device access request and inputs/outputs user data from/to a client
11 computer. The disk drive comprises an internal drive key for decrypting a secret device key
12 shared with an authentication server, wherein the secret drive key is used to decrypt the device
13 access request in order to authenticate the device access request.

14 **DESCRIPTION OF THE PREFERRED EMBODIMENTS**

15 FIG. 2 shows a computer network according to an embodiment of the present invention
16 as comprising a plurality of interconnected network devices including a plurality of client
17 computers 18, an authentication server computer 24 operated by a system administrator 12, and a
18 disk drive 22 connected to the authentication server computer 24. FIG. 3 shows a disk drive 21
19 according to an embodiment of the present invention for use as the disk drive 22 connected to the
20 authentication server computer 24 in the computer network of FIG. 2. The disk drive 21
21 comprises an interface 28 for receiving personal authentication data 26 and user access data 30
22 from the system administrator 12, a disk 32 for storing data, and a disk controller 34 for
23 controlling access to the disk 32. An authenticator 36 within the disk drive 21, responsive to the
24 personal authentication data 26, enables the disk controller 34, and cryptographic circuitry 38
25 within the disk drive 21 encrypts the user access data 30 received from the authentication server
26 computer 24 into encrypted data 40 stored on the disk 32.

27 In one embodiment, the user access data 30 comprises a plurality of user identifiers and

1 corresponding access rights to the plurality of network devices. The user identifier may be, for
2 example, a user id, and the access rights may be, for example, read/write access to a particular
3 file or partition of a disk drive connected to the network. The user access data 30 may also
4 comprise user authentication data, such as a user password.

5 In the embodiment of FIG. 2, the system administrator 12 is responsible for managing the
6 user access data for the network which is stored in encrypted form on the disk drive 22 in a
7 central database. Before allowing modifications to the central database, the system administrator
8 12 is first authenticated by transmitting personal authentication data 30 to the disk drive 22. In
9 one embodiment, the personal authentication data 30 comprises a user password known only to
10 the system administrator 12. The password is entered into a keyboard (not shown), and
11 transmitted via the authentication server computer 24 to the disk drive 22 as the personal
12 authentication data 26. The authenticator 36 (FIG. 3) within the disk drive 22 evaluates the
13 password in order to authenticate the system administrator 12, for example, by comparing the
14 received password to a password stored locally.

15 Implementing the authentication service within the disk drive 22 is safer than
16 implementing the service at the operating system level of an authentication server as in the prior
17 art network of FIG. 1. The disk drive 22 is less susceptible to virus attacks because the firmware
18 implemented by the disk controller 34 is essentially static, as determined by the manufacturing
19 process, and facilities can be employed to monitor the firmware for tampering. For example, in
20 one embodiment the firmware is stored with CRC check bytes which are used to verify that the
21 firmware has not been modified before execution. In another embodiment, the cryptographic
22 circuitry 38 and associated cryptographic keys comprise tamper-resistant circuitry embedded
23 within an integrated circuit (IC). An example discussion of tamper-resistant circuitry is provided
24 in Tygar, J.D. and Yee, B.S., "Secure Coprocessors in Electronic Commerce Applications,"
25 Proceedings 1995 USENIX Electronic Commerce Workshop, 1995, New York, which is
26 incorporated herein by reference.

27 In one embodiment, the cryptographic circuitry 38 comprises an immutable secret drive

1 key configured during manufacture of the disk drive, wherein the secret drive key is used to
2 encrypt the user access data 30. This embodiment enhances security by protecting against
3 discovery of the secret drive key through human error, that is, by obviating the need for the
4 system administrator 12 to configure the secret drive key. If an attacker steals the disk drive 22,
5 the user access data stored on the disk 32 is protected from discovery by protecting the secret
6 drive key using tamper-resistant circuitry or other similar protective measures.

7 In another embodiment, the disk 32 stores encrypted device access data associated with
8 network devices connected to a network. The device access data is used to authenticate device
9 access requests transmitted from client computers to the network devices. In one embodiment,
10 the encrypted device access data comprises an encrypted secret device key shared with a
11 corresponding network device. In one embodiment, the device access data is initially configured
12 by a system administrator 12. Unencrypted device access data is supplied to the disk drive 21
13 through its interface 28, encrypted by the cryptography circuitry 38 to generate encrypted device
14 access data, and the encrypted device access data is written to the disk 32. In an alternative
15 embodiment, the encrypted device access data is stored on the disk 32 during manufacture of the
16 disk drive 21. This embodiment enhances security by protecting against discovery of the secret
17 device keys through human error, that is, by obviating the need for the system administrator 12
18 to configure the secret device keys. In yet another embodiment, the encrypted device access data
19 is transmitted from a network device to the disk drive 21 when the network device is added to the
20 network.

21 FIG. 4 shows a disk drive 23 for use in a computer network according to another
22 embodiment of the of the present invention. The disk drive 23 comprises an interface 42 for
23 receiving from a client computer a user ID and a user access request 44 to access a network
24 device, and for transmitting device access data 46 to the client computer. The disk drive 23
25 further comprises a disk 48 for storing encrypted data, and a disk controller 50, responsive to the
26 user ID and user access request 44, for controlling access to the disk 48. Cryptographic circuitry
27 52 within the disk drive 23 decrypts the encrypted data stored on the disk 48 to generate

1 decrypted data, and the disk controller 50 uses the decrypted data to generate the device access
2 data 46 transmitted to the client computer.

3 In an embodiment shown in FIG. 2, the disk drive 23 of FIG. 4 is a disk drive 22
4 connected to an authentication server computer 24, and the client computer 18 communicates
5 with the authentication server computer 24 through network routing facilities 10. For example,
6 the client computer 18 may desire access to a server 54 connected to the network. The server 54
7 comprises a computer 56 and a disk drive 58 connected to the computer 54. In order to access
8 the server 54, the user 16 operating the client computer 18 sends a user ID and an access request
9 44 through the network routing facilities 10 to the authentication server computer 24, and
10 ultimately to the disk drive 22 connected to the authentication server computer 24. The disk
11 drive 22 (disk drive 23 of FIG. 4) stores encrypted user authentication data on the disk 48
12 corresponding to the user ID received from the client computer 18. The cryptography circuitry
13 52 within the disk drive 22 decrypts the encrypted user authentication data stored on the disk 48
14 to generate decrypted user authentication data, and the disk controller 50 uses the decrypted user
15 authentication data to generate device access data 46 transmitted to the client computer 18 for use
16 in accessing the server 54.

17 In one embodiment, the encrypted user authentication data comprises an encrypted user
18 password corresponding to the user ID received from the user 16. The disk controller 52 reads
19 the encrypted user password from the disk 48 corresponding to the user ID. The cryptographic
20 circuitry 52 decrypts the encrypted user password to generate a decrypted user password, and the
21 decrypted user password is used to generate the device access data 46 transmitted to the client
22 computer 18.

23 In one embodiment, the cryptographic circuitry 52 encrypts the device access data 46
24 before transmission to the client computer 18. In one embodiment, the cryptographic circuitry 52
25 encrypts the device access data using a cryptographic user key extracted from the decrypted user
26 authentication data (e.g., the decrypted user password). In one embodiment, the cryptographic
27 user key is generated by the cryptographic circuitry 52 using the decrypted authentication data

(e.g., the decrypted user password). In one embodiment, the cryptographic user key is a private key for use in a private key encryption algorithm (symmetric algorithm), and in an alternative embodiment the cryptographic user key is a public key for use in a public key encryption algorithm (asymmetric algorithm).

The encrypted device access data 46 can only be decrypted with a user key associated with the user ID and known only to the trusted user having been assigned the user ID. In one embodiment, the client computer 18 generates the user key using a password provided by the user 16. Thus, the user key can only be generated if the user 16 operating the client computer 18 is in possession of the trusted password.

In one embodiment, the cryptographic circuitry 52 encrypts the device access data using a secret device key shared with the network device, where the secret device key is used by the network device to authenticate device access requests received from client computers. In one embodiment, the secret device key shared with the network device is stored in encrypted form on the disk 48 and decrypted by the cryptographic circuitry 52.

In yet another embodiment, the cryptographic circuitry 52 comprises an immutable secret drive key configured during manufacture of the disk drive, wherein the secret drive key is used to decrypt the encrypted data stored on the disk 48. Similar to the embodiment described above with reference to FIG. 3, this embodiment enhances security by protecting against discovery of the secret drive key through human error, that is, by obviating the need for the system administrator 12 to configure the secret drive key. If an attacker steals the disk drive 22, the data stored on the disk 32 is protected from discovery by protecting the secret drive key using tamper-resistant circuitry or other similar protective measures.

FIG. 5 shows a disk drive 60 for use in a computer network according to another embodiment of the of the present invention. The disk drive 60 comprises an interface 62 for receiving an encrypted device access request 64 and for inputting/outputting user data 66 from/to a client computer, a disk 68 for storing data, and a disk controller 70 for controlling access to the disk 68. The disk drive 60 further comprises an internal drive key 72, and a secret device key

1 shared with an authentication server, the secret device key stored in encrypted form.
2 Cryptographic circuitry 74, responsive to the internal drive key 72, decrypts the encrypted secret
3 device key to generate a decrypted secret device key, and an authenticator 76, responsive to the
4 decrypted secret device key, authenticates the device access request 64.

5 In an embodiment illustrated in FIG. 2, the disk drive 60 of FIG. 5 is a disk drive
6 connected to a network (e.g., disk drive 58 connected to a server computer 56 or a disk drive
7 connected directly to the network as a network attached storage device (NASD)). The secret
8 device key within the disk drive 58 is shared with an authentication server and used to
9 authenticate user access requests. The authentication server uses the secret device key to encrypt
10 device access data transmitted to a client computer 18 requesting access to the disk drive 58, and
11 the disk drive 58 uses the secret device key to authenticate access requests received from the
12 client computer 18.

13 In one embodiment, the secret device key is stored in encrypted form on the disk 68.
14 When a device access request is received from a client computer, the disk controller reads the
15 encrypted secret device from the disk 68 and the cryptography circuitry 74 decrypts the
16 encrypted secret drive key to generate the decrypted secret drive key used to authenticate the
17 device access request.

18 In another embodiment, the encrypted secret device key is configured during manufacture
19 of the disk drive 60, and the disk drive 60 transmits the encrypted secret device key to the
20 authentication server when the disk drive 60 is added to the network (e.g., added as drive 58 in
21 FIG. 2). This embodiment enhances the security of the authentication service by avoiding
22 discovery through human error, that is, by obviating the need for a system administrator 12 to
23 configure the secret device key. In another embodiment, the internal drive key 72 comprises
24 tamper-resistant circuitry which protects against an attacker who probes the disk drive 60
25 attempting to discover the secret device key.

1 **WE CLAIM:**

- 1 1. A computer network comprising a plurality of interconnected network devices including:
2 (a) a plurality of client computers;
3 (b) an authentication server computer operated by a system administrator; and
4 (c) a disk drive connected to the authentication server computer, the disk drive
5 comprising:
6 an interface for receiving personal authentication data and user access data from the
7 system administrator;
8 a disk for storing data;
9 a disk controller for controlling access to the disk;
10 an authenticator, responsive to the personal authentication data, for enabling the disk
11 controller; and
12 cryptographic circuitry for encrypting the user access data received from the system
13 administrator into encrypted data stored on the disk.
- 1 2. The computer network as recited in claim 1, wherein the user access data comprises a
2 plurality of user identifiers and corresponding access rights to the plurality of network
3 devices.
- 1 3. The computer network as recited in claim 2, wherein the user access data further
2 comprises user authentication data.
- 1 4. The computer network as recited in claim 3, wherein the user authentication data
2 comprises a user password.
- 1 5. The computer network as recited in claim 1, wherein the personal authentication data
2 comprises a user password.

6. The computer network as recited in claim 1, wherein:

- (a) the cryptographic circuitry comprises an immutable secret drive key configured during manufacture of the disk drive; and
- (b) the secret drive key for use in encrypting the user access data.

7. The computer network as recited in claim 2, wherein:

- (a) the disk stores encrypted device access data associated with the network devices; and
- (b) the device access data for use in authenticating device access requests transmitted from client computers to the network devices.

8. The computer network as recited in claim 7, wherein the encrypted device access data comprises an encrypted secret device key shared with a corresponding network device.

9. The computer network as recited in claim 7, wherein:

- (a) the interface receives unencrypted device access data; and
- (b) the cryptographic circuitry encrypts the unencrypted device access data into the encrypted device access data stored on the disk.

10. The computer network as recited in claim 7, wherein the encrypted device access data is stored on the disk during manufacture of the disk drive.

11. The computer network as recited in claim 7, wherein the encrypted device access data is transmitted from the network devices to the disk drive.

12. A computer network comprising a plurality of interconnected network devices including:

(a) a plurality of client computers;

(b) an authentication server computer; and

(c) a disk drive connected to the authentication server computer, the disk drive comprising:

an interface for receiving from a client computer a user ID and a user access request to access a network device, and for transmitting device access data to the client computer;

a disk for storing encrypted data;

a disk controller, responsive to the user ID and user access request, for controlling access to the disk; and

cryptographic circuitry for decrypting the encrypted data stored on the disk to generate decrypted data,

wherein the disk controller uses the decrypted data to generate the device access data transmitted to the client computer.

13. The computer network as recited in claim 12, wherein:

(a) the encrypted data comprises encrypted user authentication data corresponding to the user ID; and

(b) the cryptographic circuitry decrypts the encrypted user authentication data to generate decrypted user authentication data.

14. The computer network as recited in claim 13, wherein the decrypted user authentication data comprises a user password.

15. The computer network as recited in claim 12, wherein the cryptographic circuitry encrypts the device access data before transmission to the client computer.

1 16. The computer network as recited in claim 13, wherein:

2 (a) the cryptographic circuitry encrypts the device access data before transmission to the
3 client computer; and

4 (b) the cryptographic circuitry encrypts the device access data using a cryptographic user
5 key extracted from the decrypted user authentication data.

1 17. The computer network as recited in claim 16, wherein the cryptographic user key is
2 generated by the cryptographic circuitry using the decrypted user authentication data.

3 18. The computer network as recited in claim 16, wherein the cryptographic user key is a
4 public key for use in a public key encryption algorithm.

5 19. The computer network as recited in claim 12, wherein:

6 (a) the cryptographic circuitry encrypts the device access data using a secret device key
7 shared with the network device; and

8 (b) the secret device key is used by the network device to authenticate device access
9 requests received from client computers.

1 20. The computer network as recited in claim 19, wherein the secret device key shared with
2 the network device is stored in encrypted form on the disk and decrypted by the
3 cryptography circuitry.

4 21. The computer network as recited in claim 12, wherein:

5 (c) the cryptographic circuitry comprises an immutable secret drive key configured
6 during manufacture of the disk drive; and

7 (d) the secret drive key for use in decrypting the encrypted data stored on the disk.

22. A computer network comprising a plurality of interconnected network devices including:

(a) a plurality of client computers;

(b) an authentication server; and

(c) a disk drive comprising:

an interface for receiving an encrypted device access request and for

inputting/outputting user data from/to a client computer;

a disk for storing data;

a disk controller for controlling access to the disk;

an internal drive key;

a secret device key shared with the authentication server, the secret device key stored
in encrypted form;

cryptographic circuitry, responsive to the internal drive key, for decrypting the

encrypted secret device key to generate a decrypted secret device key; and

an authenticator, responsive to the decrypted secret device key, for authenticating the
device access request.

23. The computer network as recited in claim 22, wherein the encrypted secret device key is
stored on the disk.

24. The computer network as recited in claim 22, wherein the encrypted secret device key is
configured during manufacture of the disk drive.

25. The computer network as recited in claim 22, wherein the disk drive transmits the
encrypted secret device key to the authentication server.

26. The computer network as recited in claim 22, wherein the internal drive key comprises

2 tamper-resistant circuitry.

09/20/00 09:20:00

A COMPUTER NETWORK COMPRISING NETWORK AUTHENTICATION FACILITIES IMPLEMENTED IN A DISK DRIVE

ABSTRACT OF THE DISCLOSURE

A computer network is disclosed comprising a plurality of interconnected network devices including a plurality of client computers, an authentication server computer operated by a system administrator, and a disk drive connected to the authentication server computer. The disk drive comprises an interface for receiving the personal authentication data and user access data from the system administrator, a disk for storing data, and a disk controller for controlling access to the disk. An authenticator within the disk drive, responsive to the personal authentication data, enables the disk controller, and cryptographic circuitry encrypts the user access data received from the system administrator into encrypted data stored on the disk.

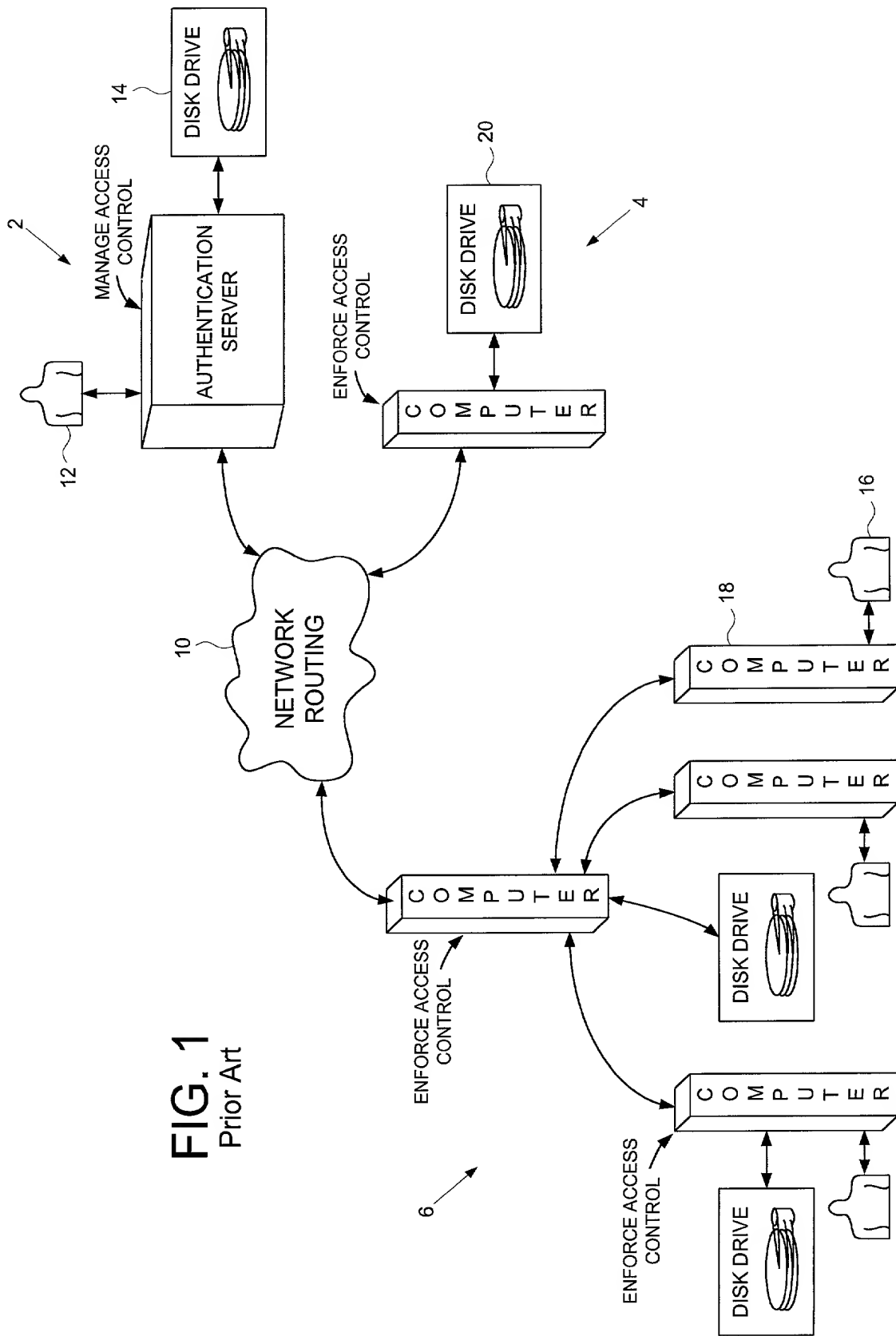
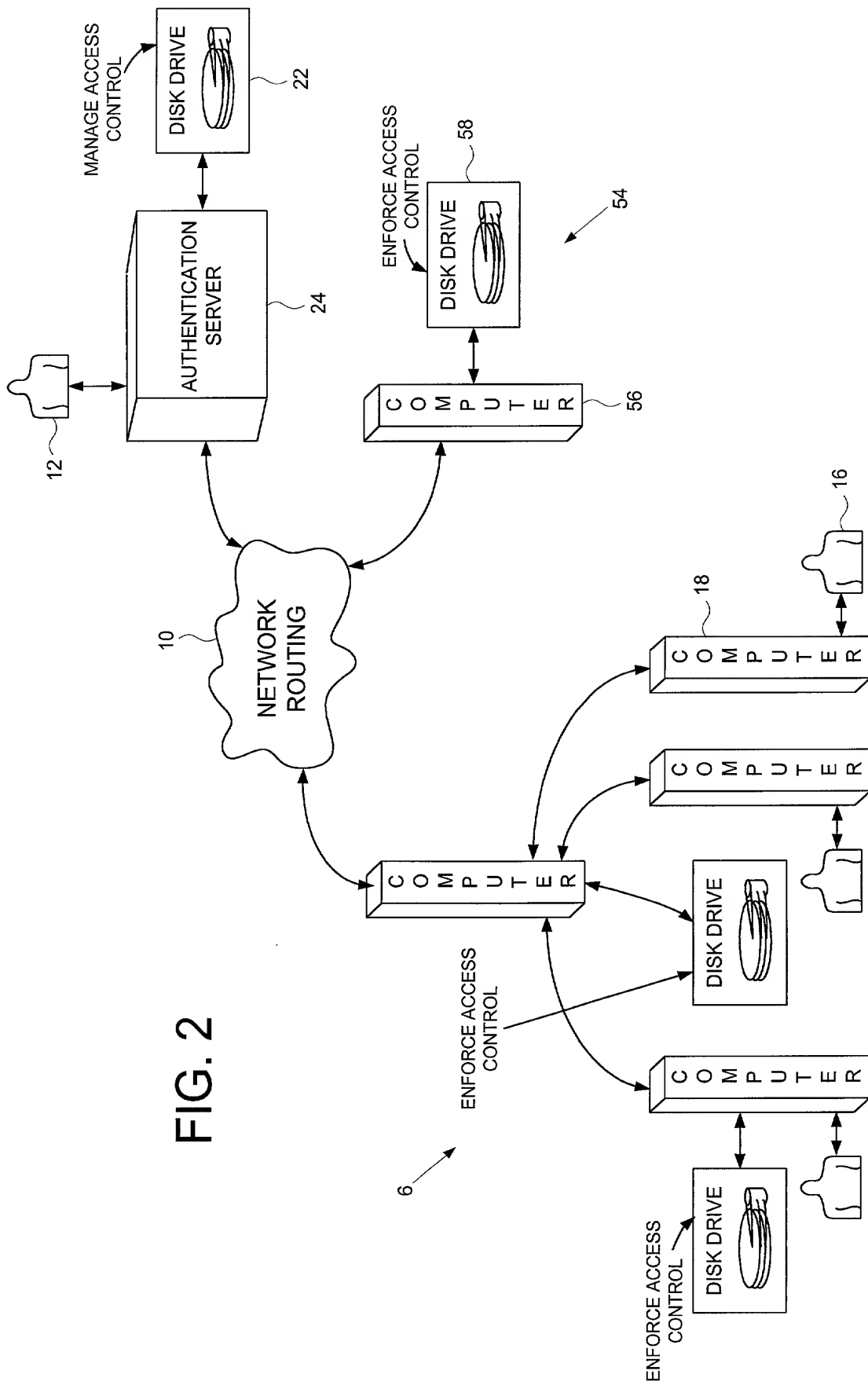


FIG. 1
Prior Art



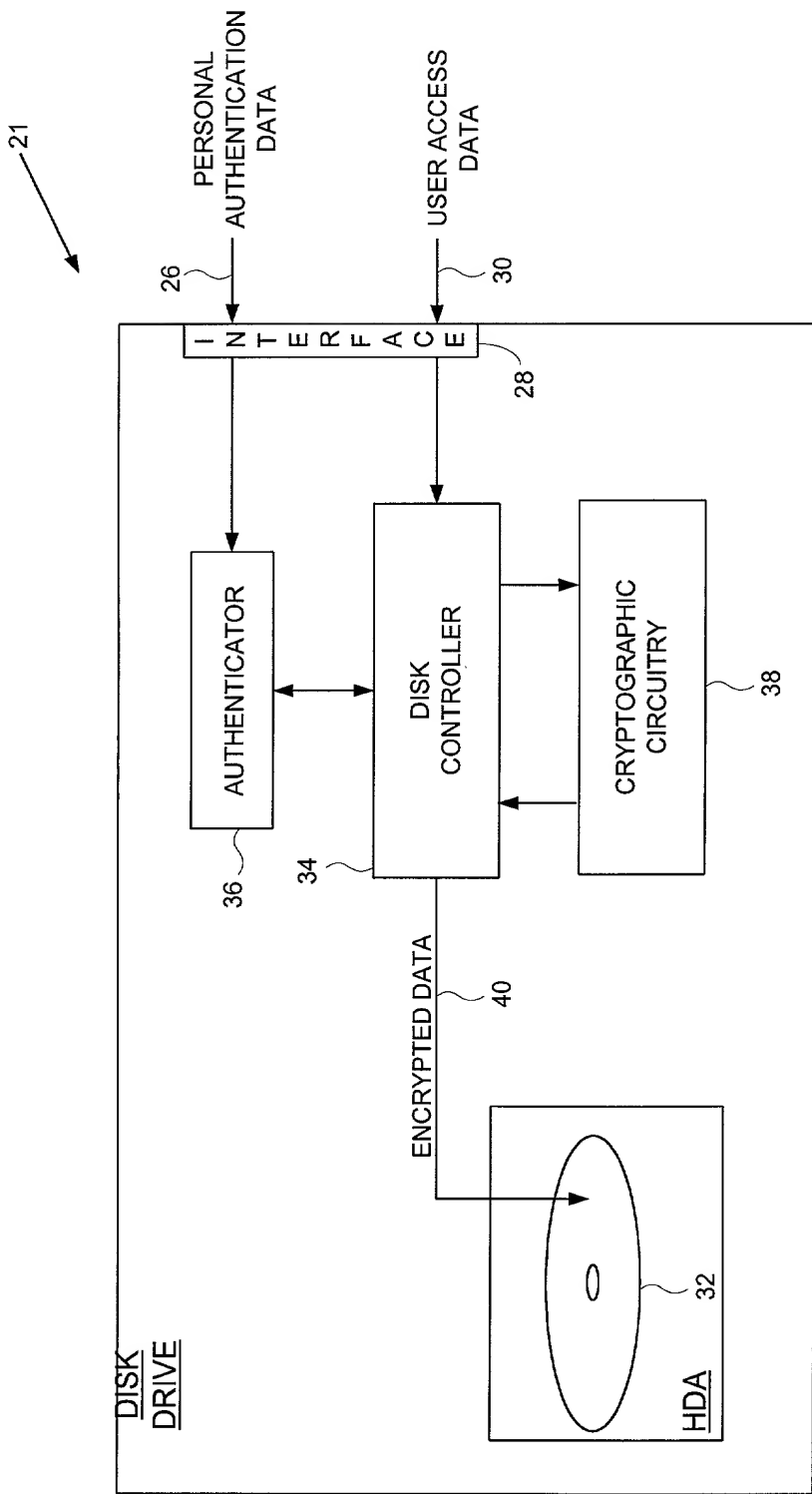


FIG. 3

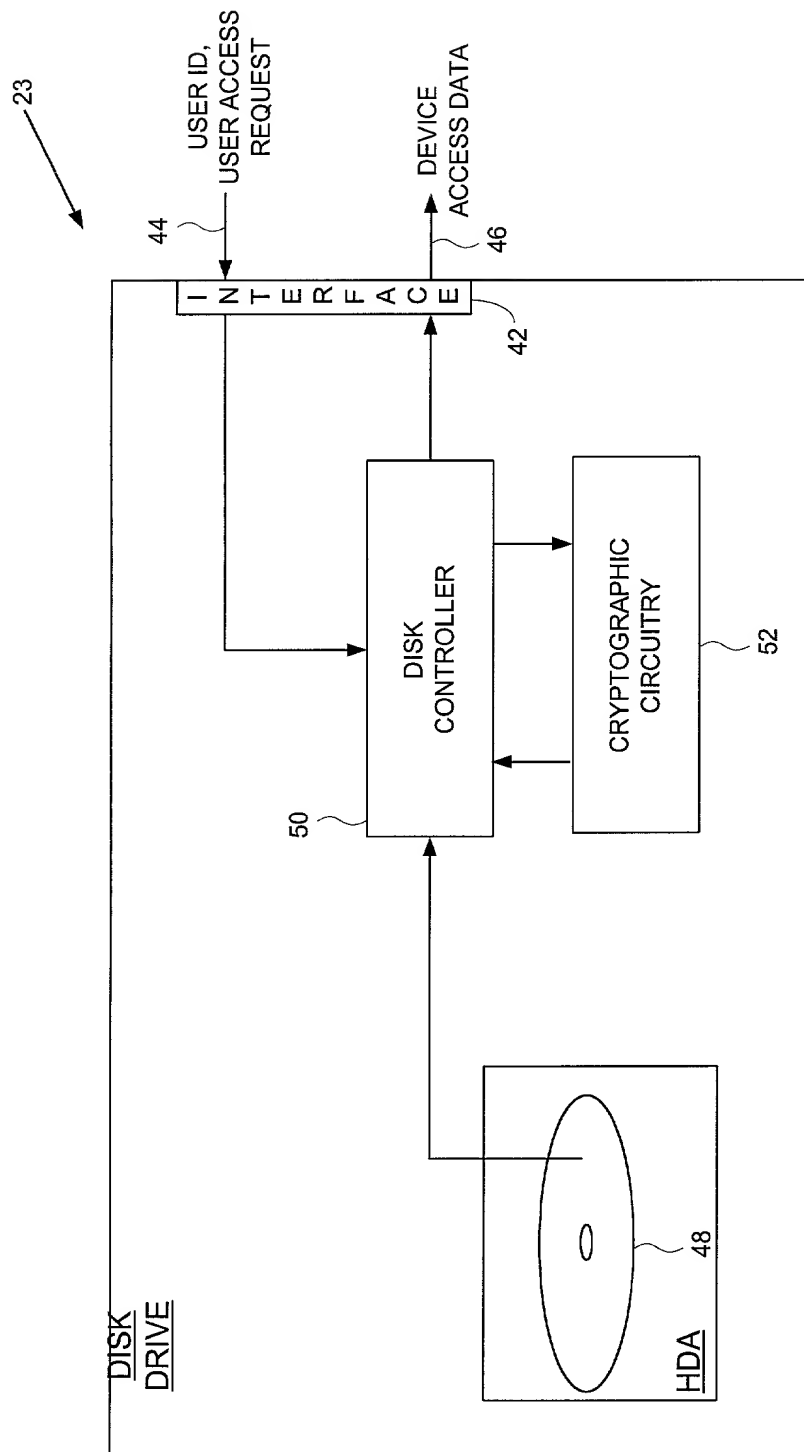


FIG. 4

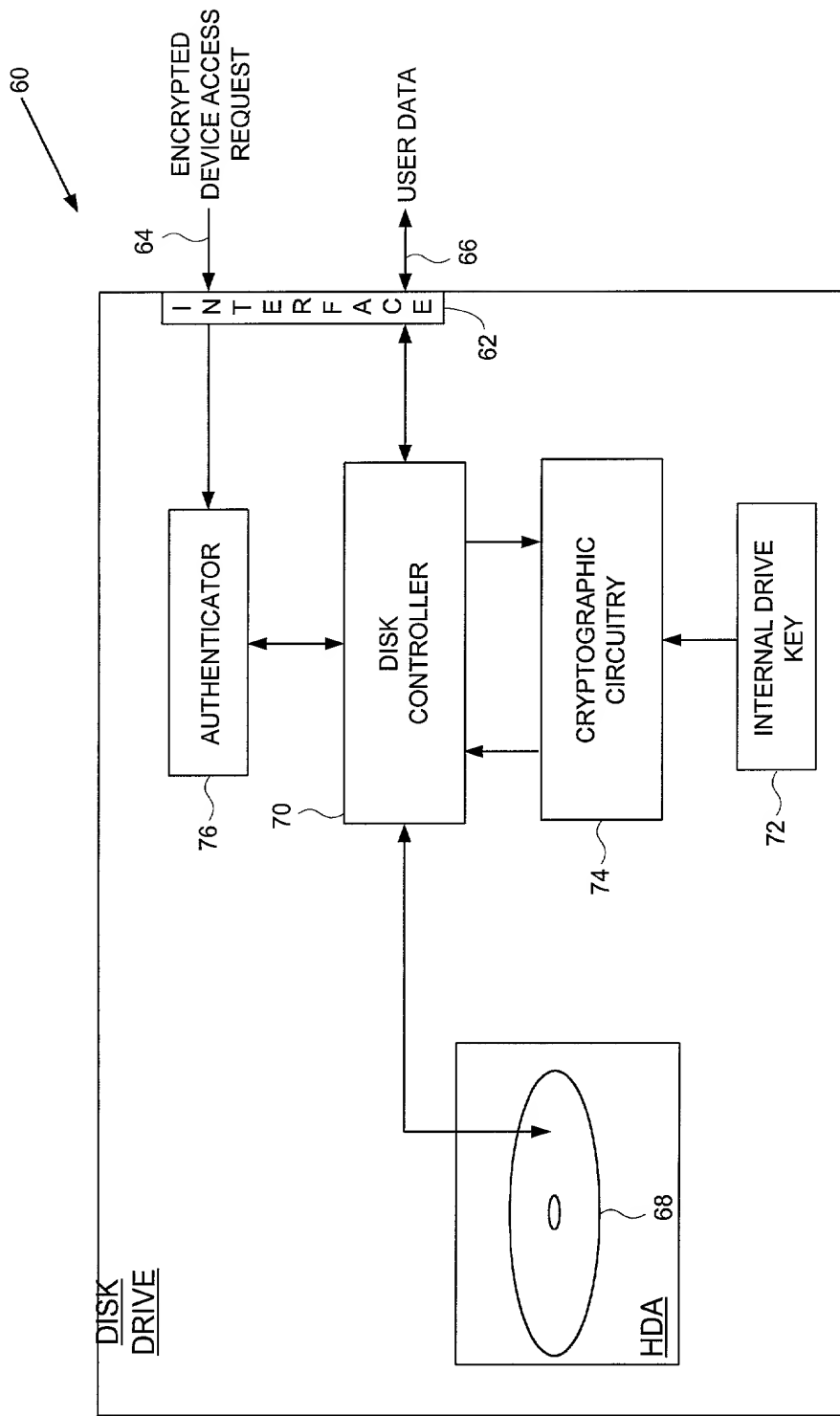


FIG. 5